Sean K. Claggett, Esq.
Nevada Bar No. 8407
Matthew S. Granda, Esq.
Nevada Bar No. 12753
Micah S. Echols, Esq.
Nevada Bar No. 8437
David P. Snyder, Esq.
Nevada Bar No. 15333
Charles L. Finlayson, Esq.
Nevada Bar No. 13685
CLAGGETT & SYKES LAW FIRM
4101 Meadows Ln., Ste. 100
Las Vegas, Nevada 89107
(702) 655-2346 – Telephone
(702) 655-3763 – Facsimile
sclaggett@claggettlaw.com
micah@claggettlaw.com
charlie@claggettlaw.com

David M. Berger (*pro hac vice to be submitted*)
Jeffrey B. Kosbie (*pro hac vice to be submitted*)
Julia L. Gonzalez (*pro hac vice to be submitted*)
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9700
Facsimile: (510) 350-9701
dmb@classlawgroup.com
jbk@classlawgroup.com
jlg@classlawgroup.com

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

MICHAEL CARROZZELLA, FRANK ANDERSON, AND GREG LEWIS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, **PLAINTIFFS,** **v.** **CAESARS ENTERTAINMENT, INC.,** **DEFENDANT**	**CASE NO.** **CLASS ACTION** **COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY, AND INJUNCTIVE RELIEF** **JURY DEMAND**

Plaintiffs Michael Carrozzella, Frank Anderson, and Greg Lewis, individually and on behalf of all others similarly situated, bring this action against Caesars Entertainment for damages and equitable, declaratory, and injunctive relief. Plaintiffs allege as follows:

INTRODUCTION

1. On September 14, 2023, Caesars Entertainment announced that hackers had stolen a copy of its loyalty program database, containing the Personally Identifiable Information ("PII") of Caesars loyalty program members, including Social Security and driver's license numbers for a "significant number" of members ("Caesars Data Breach").[1]

2. According to its public filings, the hackers infiltrated Caesars' networks on August 18, 2023, and began exfiltrating data approximately five days later. But Caesars did not discover the breach until September 7, 2023.[2]

3. Caesars has disclosed that over 40,000 residents in the state of Maine alone had data stolen in the breach,[3] which suggests the Caesars breach likely affected many millions of people across the country.

4. Caesars prides itself on being the largest gaming company in the United States. Caesars also runs the largest casino loyalty program in the United States with over 60 million members, which it calls Caesars Rewards.[4]

5. Caesars Rewards members share their personal information with Caesars, expecting it will keep the data safe and not expose it to the world.

6. Caesars, in turn, provides special benefits to Caesars Rewards members in selling them its goods and services. The more that members spend on Caesars' goods and services, the higher "Tier" of membership they can achieve.[5]

7. The Caesars Data Breach was a direct result of Caesars' failure to implement adequate and

---

[1] https://response.idx.us/Caesars/#learn-more.
[2] https://apps.web.maine.gov/online/aeviewer/ME/40/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml
[3] https://apps.web.maine.gov/online/aeviewer/ME/40/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml
[4] https://www.Caesars.com/corporate; https://www.vegashowto.com/caesars-rewards
[5] https://www.caesars.com/myrewards/benefits-overview; https://www.caesars.com/content/dam/caesars-rewards/benefits/2023-07-cr-flipbook-reprint-czr.pdf

reasonable cyber-security procedures and protocols necessary to protect members' PII.

8. Plaintiffs, individually and on behalf of all others similarly situated, allege claims under the Nevada Consumer Fraud Act (Nev. Rev. Stat. § 41.600), the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200), the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq.*), the California Consumer Records Act (Cal. Civ. Code § 1798.80, *et seq.*), and for negligence, negligent misrepresentation, and unjust enrichment. Plaintiffs, individually and on behalf of all others similarly situated ask the Court to compel Caesars to adopt information security practices that are reasonable for the vast amounts of sensitive PII that Caesars warehouses in its databases, to prevent an incident like the Caesars Data Breach from recurring, and to grant such other relief as the Court deems just and proper.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The putative class contains millions of members, many of whom have citizenship diverse from Caesars.

10. This Court has jurisdiction over Caesars because its principal place of business is in the District of Nevada, it operates in this District, and the computer systems implicated in the Caesars Data Breach are likely based in this District. Through its business operations in this District, Caesars intentionally avails itself of the markets within this District such that the exercise of jurisdiction by this Court is just and proper.

11. Venue is proper under 28 U.S.C. § 1391(b)(1) because Caesars resides in Nevada. Venue is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to this action occurred in this District. Caesars is based in this District, maintains customer PII in the District, and has caused harm to Plaintiffs and Class members residing in this District.

PARTIES

12. Plaintiff Frank Anderson is a resident and citizen of Nevada. He has been a Caesars Rewards member for approximately 10 years. During that time, Mr. Anderson has used Caesars services, often several times per year, and he has provided his PII to Caesars in connection with using those services.

To become a member of Caesars Rewards, Mr. Anderson provided PII to Caesars including his full name, address, date of birth, driver's license number, and Social Security number.

13. Mr. Anderson is aware of Caesars' statement that a copy of its customer loyalty database has been obtained by the hackers, which would have included Mr. Anderson's PII. As a consequence of the Caesars Data Breach, Mr. Anderson has been forced to spend time monitoring his financial accounts and credit, researching the data breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft, among other harms. Because Caesars has not notified Mr. Anderson or other Rewards program members of the full extent of the Data Breach, Mr. Anderson has been forced to take reasonable measures to mitigate the harm on his own.

14. Plaintiff Michael Carrozzella is a resident and citizen of California. He has been a Caesars Rewards member for approximately 10 years. During that time, Mr. Carrozzella has stayed at Caesars properties and used Caesars services, often several times per year, and he has provided his PII to Caesars in connection with staying at those properties and using those services. To become a member of Caesars Rewards, Mr. Carrozzella provided PII to Caesars including his full name, address, date of birth, driver's license number, and Social Security number.

15. On or around October 19, 2023, Mr. Carrozzella received a data breach notification from Caesars informing him that his PII was compromised in the data breach. In addition, Mr. Carrozzella is aware of Caesars' statement that a copy of its customer loyalty database has been obtained by the hackers. As a consequence of the Caesars Data Breach, Mr. Carrozzella has been forced to take reasonable measures to mitigate the harm, including spend time monitoring his financial accounts and credit, researching the data breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft, among other harms.

16. Plaintiff Greg Lewis is a resident and citizen of Kentucky. He has been a Caesars Rewards member for over three years and has reached "Diamond Elite" membership status, which is the second highest of the six membership statuses. During that time, Mr. Lewis has stayed at Caesars properties and used Caesars services, often several times per year, and he has provided his PII to Caesars in connection with staying at those properties and using those services. To become a member of Caesars Rewards, Mr.

Lewis provided PII to Caesars including his full name, address, date of birth, driver's license number, and Social Security number.

17. On or around October 19, 2023, Mr. Lewis received a data breach notification from Caesars informing him that his PII was compromised in the data breach. In addition, Mr. Lewis is aware of Caesars' statement that a copy of its customer loyalty database has been obtained by the hackers. As a consequence of the Caesars Data Breach, Mr. Lewis has been forced to take reasonable measures to mitigate the harm, including spend time monitoring his financial accounts and credit, researching the data breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft, among other harms. In particular, after he learned about the data breach, Mr. Lewis both enrolled in a credit monitoring and identity protection service and also updated his passwords in order to prevent and mitigate the likelihood of identity theft.

18. As a result of the Caesars Data Breach, Plaintiffs and Class members have suffered actual injuries including: (a) paying monies to Caesars for its goods and services, which Plaintiffs would not have done had Caesars disclosed that it lacked data security practices adequate to safeguard Plaintiffs' PII from theft; (b) damages to and diminution in the value of Plaintiffs' PII—a form of property that Plaintiffs entrusted to Caesars as a condition of receiving its services; (c) loss and invasion of Plaintiffs' privacy; and (d) injuries arising from the increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protections measures, which will continue for years.

19. Defendant Caesars Entertainment is a Delaware corporation headquartered at 100 West Liberty Street, 12th Floor, Reno, Nevada 89501. Caesars is a global gaming and hospitality company that owns, leases, brands or manages 53 domestic properties across 18 states with approximately 52,700 slot machines and 47,200 hotel rooms.[6] It also operates and conducts sports wagering across 30 jurisdictions in North America.[7] Its notable properties and services include Caesars Palace, Caesars Sportsbook, Caesars Racebook, Harrah's hotel, Paris Las Vegas, Planet Hollywood, Flamingo Las Vegas, and The Linq.

[6] https://www.sec.gov/ix?doc=/Archives/edgar/data/1590895/000159089523000091/czr-20230630.htm
[7] https://www.sec.gov/ix?doc=/Archives/edgar/data/1590895/000159089523000091/czr-20230630.htm

STATEMENT OF FACTS

I. The Data Breach

20. According to Caesars, hackers first gained access to its network on August 18, 2023, and began exfiltrating data by August 23.[8] Caesars did not realize that the hackers had acquired a copy of its loyalty program database and other data until September 7, 2023.[9]

21. On September 14, 2023, Caesars filed a Form 8-K with the SEC stating that it had "identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company" and had, on September 7, "determined that the unauthorized actor acquired a copy of, among other data, [its] loyalty program database, which includes driver's license numbers and/or Social Security numbers for a significant number of members in the database."[10] Caesars posted a notice conveying the same information on its website.[11]

22. On October 6, 2023, Caesars filed a data breach notification with the Office of the Maine Attorney General.[12] In the Maine data breach notification, Caesars identified the total number of impacted individuals as "TBD," but specified the number of impacted residents of the state of Maine as 41,397, and it provided a copy of the template data breach notice it would provide to those residents.[13]

23. The template notice says that names and other unspecified "data elements" were compromised.[14]

II. Caesars' Privacy Promises

24. Caesars' Privacy Policy states that it is "committed to respecting your data privacy" and that it maintains "physical, electronic, and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of information under our control."[15]

25. Members' personal data is valuable to Caesars for profit-generating purposes, including

---

[8] https://apps.web.maine.gov/online/aeviewer/ME/40/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml
[9] https://www.sec.gov/Archives/edgar/data/1590895/000119312523235015/d537840d8k.htm
[10] https://www.sec.gov/Archives/edgar/data/1590895/000119312523235015/d537840d8k.htm
[11] https://response.idx.us/caesars/#learn-more
[12] https://apps.web.maine.gov/online/aeviewer/ME/40/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml
[13] https://apps.web.maine.gov/online/aeviewer/ME/40/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml
[14] https://apps.web.maine.gov/online/aeviewer/ME/40/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml
[15] https://www.caesars.com/corporate/privacy

marketing products and services "provided by us or our affiliates or other third parties."[16]

26. Despite its assurances, Caesars failed to maintain the necessary security measures, practices, and other safeguards that would have prevented the Caesars Data Breach.

III. Caesars Knew It Was a Prime Target

27. Caesars knew that the massive databases of PII it collected, processed, and stored were tantalizing targets for hackers.[17]

28. Hotel and hospitality companies are particularly attractive targets for financially-motivated hackers looking steal PII. Trustwave's *2020 Global Security Report* lists hospitality as the industry with the third largest share of security compromises and data breaches.[18] Indeed, "The hospitality industry is a common target for cyber criminals because of the massive amount of data hotels hold."[19]

29. Caesars was particularly aware that it was a prime target for data breaches because of past attacks affecting other large gambling enterprises. In July 2019, hackers gained unauthorized access to MGM's networks, successfully exfiltrating PII of millions of MGM's customers.

IV. Caesars Failed to Comply with Established Cybersecurity Frameworks and Industry Standards

30. The Federal Trade Commission ("FTC") has promulgated various guides for businesses, which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

31. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide

---

[16] https://www.caesars.com/corporate/privacy

[17] Identity Theft Resource Center, *Identity Theft Resource Center's 2022 Annual Data Breach Report Reveals Near-Record Number of Compromises*, https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/

[18] *2020 Trustwave Global Security Report*, https://21158977.fs1.hubspotusercontent-na1.net/hubfs/21158977/Web/Library/Documents%20pdf/D_16791_2020-trustwave-global-security-report.pdf

[19] Open Data Security, *Cybersecurity in the Hotel Industry: Lessons from Marriott Data Breach*, https://opendatasecurity.io/cybersecurity-in-the-hotel-industry-lessons-from-marriott-data-breach/.

[20] *See Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, *available* at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

for Business, which established cyber-security guidelines for businesses.[21] The guidelines state that:

a) Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it";

b) Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c) Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d) Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e) Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.

32. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[22]

33. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

34. Orders from FTC enforcement actions further clarify the measures businesses must take to meet their data security obligations.

35. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

---

[21] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, October 2016, *available* at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

[22] *See Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, *available* at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

36. Caesars' failure to adopt reasonable safeguards to protect PII constitutes an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45, and state statutory analogs.

37. Similarly, the U.S. Government's National Institute of Standards and Technology (NIST) provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[23]

38. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[24] Caesars failed to adhere to the NIST guidance.

39. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the hotel industry, including the following:

a) Installing appropriate malware detection software;

b) Monitoring and limiting network ports;

c) Protecting web browsers and email management systems;

d) Setting up network systems such as firewalls, switches, and routers;

e) Monitoring and protecting physical security systems; and

f) Training hotel staff regarding critical points.[25]

40. Caesars' failure to protect massive amounts of PII is a result of its failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

41. Caesars was well aware of its obligations to use reasonable measures to protect consumers' PII. Caesars also knew it was a target for hackers, as discussed above. Despite understanding the risks and consequences of inadequate data security, Caesars failed to comply with its data security obligations.

///

---

[23] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, *available* at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

[24] *Id.* at Table 2 pg. 26-43.

[25] *See How to Work on Hotel Cyber Security*, Open Data Security, July 23, 2019, *available* at https://opendatasecurity.io/how-to-work-on-hotel-cyber-security/

V. The Caesars Data Breach Harmed Individuals, And Additional Fraud Will Result

42. Consumers who have been victims of data breaches are much more likely to become victims of identity fraud than those who have not. Further, each additional data breach an individual is involved in increases his or her risk of identity fraud.

43. As the FTC explains, "[o]nce identity thieves steal your personal information . . . they can drain your bank account, run up charges on your credit cards, get new credit cards in your name, open a phone, cable, or other utility account in your name, steal your tax refund, use your health insurance to get medical care, or pretend to be you if they are arrested."[26] As such, PII is a highly valuable asset to ill-intending identity thieves.

44. The U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[27]

45. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.[28]

46. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding

[26] https://consumer.ftc.gov/articles/free-credit-reports
[27] Erika Harrell, *Victims of Identity Theft, 2014*, NCJ 248991, September, 27, 2015, *available* at https://bjs.ojp.gov/content/pub/pdf/vit14.pdf
[28] Consumer Protection Division of the Maryland Office of the Attorney General, *Identity Theft: Protect Yourself, Secure Your Future*, https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf

> payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[29]

47. Therefore, information compromised in this Data Breach is more valuable than the loss of, for example, credit card information in a retailer data breach. There, victims can close credit and debit card accounts, typically for free. Here, the information compromised—Social Security numbers, drivers' license numbers, and names—cannot be "closed" and is difficult, if not impossible, to change.

48. Caesars is offering members of its Rewards program two years of free identity protection services, but the identity protection services Caesars is offering are inadequate protection. In fact, identity thieves often hold onto personal information in order to commit fraud years after such free programs expire. Moreover, the services Caesars is offering fail to actually *prevent* identity theft. At best, they can report after the theft occurs. Moreover, the insurance and other benefits that Caesars offers is insufficient, full of coverage loopholes, and very difficult to successfully claim.

49. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

50. Plaintiffs seek relief individually and as representatives of all others similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs seek certification of a Nationwide class defined as follows:

> All persons in the United States whose personal information was compromised in the data breach publicly announced by Caesars Entertainment in September 2023.

Plaintiff Carrozzella also seeks certification of a California Subclass, defined as follows:

> All California residents whose personal information was compromised in the data breach publicly announced by Caesars Entertainment in September 2023.

51. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns.

[29] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf..

Also excluded are any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

52. **Numerosity**: Federal Rule of Civil Procedure 23(a)(1). The Class members are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Caesars has already admitted that a copy of its loyalty program database was stolen, and Caesars' loyalty program has over 60 million members. Given the overall class size and the proximity of Caesars properties to California, it is certain that there are at least several hundred thousand Subclass members. The individuals' names and addresses are available from Defendant's records.

53. **Commonality and Predominance**: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). The action involves common questions of law and fact, which predominate over any questions affecting individual class members, including:

a. Whether Defendant knew or should have known that its systems were vulnerable to unauthorized access;

b. Whether Defendant failed to take adequate and reasonable measures to ensure its data systems were protected;

c. Whether Defendant failed to take available steps to prevent and stop the breach from happening;

d. Whether Defendant owed a legal duty to Plaintiffs and Class members to protect their PII;

e. Whether Defendant breached any duty to protect the personal information of Plaintiffs and Class members by failing to exercise due care in protecting their PII;

f. Whether Plaintiffs and Class members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

g. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief or restitution.

///

///

54. **Typicality**: Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of other Class members' claims because Plaintiffs and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

55. **Adequacy of Representation**: Federal Rule of Civil Procedure 23(a)(4). Plaintiffs are adequate class representatives because their interests do not conflict with the interests of the Class they seek to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation and data breach litigation, and Plaintiffs intend to prosecute this action vigorously. Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

56. **Declaratory and Injunctive Relief**: Federal Rule of Civil Procedure 23(b)(2). The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

57. **Superiority**: Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this case. Relative to the burden and expense that would be required to individually litigate the claims, the damages suffered by Plaintiffs and Class members are comparatively small, so it would be impracticable for them to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

58. Caesars has physical and email addresses for Class members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

COUNT I

VIOLATION OF NEVADA'S CONSUMER FRAUD ACT
Nevada Revised Statutes § 41.600
(*asserted by all Plaintiffs on behalf of the Class*)

59. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

60. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, may be applied on a nationwide basis because Caesars' unlawful conduct was centered in Nevada.

61. Caesars is subject to the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, because it is headquartered in and does business in Nevada. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, states, "1. An action may be brought by any person who is a victim of consumer fraud. 2. As used in this section, 'consumer fraud' means: . . . (e) A deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive."

62. In turn, Nev. Rev. Stat. § 598.0923(1) (part of the Nevada Deceptive Trade Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . (b) Fails to disclose a material fact in connection with the sale or lease of goods or services." The Caesars Rewards program provides benefits to its members who purchase Caesars' goods and services. Caesars violated this provision because its Privacy Policy states that it maintains physical, electronic, and organizational safeguards to protect PII under its control, and Caesars failed to disclose the material fact that its data security practices were inadequate to reasonably safeguard consumers' PII. Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hospitality industry was a frequent target of sophisticated cyberattacks. Caesars could and should have made a proper disclosure during the account creation process for its Caesars Rewards program, as part of the purchase of goods or services by Caesars

Rewards members, or by any other means reasonably calculated to inform consumers of its inadequate data security.

63. Nev. Rev. Stat. § 598.0923(1) also states that: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . (c) Violates a state or federal statute or regulation relating to the sale or lease of goods or services." Caesars committed several such violations, each of which serves as an independent act sufficient to constitute a deceptive trade practice.

64. First, Caesars breached a Nevada statue requiring reasonable data security. Specifically, Nev. Rev. Stat. § 603A.210(1), which regulates information security of businesses that collect data "for any purpose," states: "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition . . . or disclosure." Caesars is a data collector as defined at Nev. Rev. Stat. § 603A.030, and collects data for, among other purposes, marketing and selling Caesars Rewards members its goods and services. Caesars failed to implement and maintain reasonable security measures, evidenced by the fact that hackers accessed Caesars' loyalty program database and stole consumers' PII. Caesars' violation of this statute was done knowingly for purposes of Nev. Rev. Stat. § 598.0923(1) because Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hospitality industry is a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation.

65. Second, Caesars breached other state statutes regarding unfair trade practices and data security requirements as alleged *infra*. Specifically, Caesars violated the California state statutes set forth in Counts II-IV. Caesars knew or should have known that it violated these statutes. Caesars' violations of each of these statutes serves as an independent act sufficient to constitute a deceptive trade practice under Nev. Rev. Stat. § 598.0923(1).

66. Third, Caesars violated the FTC Act, 15 U.S.C. § 45, as alleged above. Caesars knew or should have known that its data security practices were deficient, violated the FTC Act, and that it failed to adhere to the FTC's data security guidance. This is true because, among other things, Caesars was aware that the hospitality industry is a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation. Caesars' violation of the FTC Act serves as an independent act sufficient to constitute a deceptive trade practice under Nev. Rev. Stat. § 598.0923(1).

67. Caesars engaged in deceptive or unfair practices by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiffs and Class members.

68. Nev. Rev. Stat. § 41.600(3) states that if the plaintiffs prevail, the court "shall award . . . (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) The claimant's costs in the action and reasonable attorney's fees."

69. As a direct and proximate result of the foregoing, Plaintiffs and Class members suffered all forms of damages alleged herein. Plaintiffs' harms constitute compensable damages for purposes of Nev. Rev. Stat. § 41.600(3).

70. Plaintiffs and Class members are also entitled to all forms of injunctive relief sought herein.

71. Plaintiffs and Class members are also entitled to an award of their attorney's fees and costs pursuant to Nev. Rev. Stat. § 41.600(3)(c).

COUNT II
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq.*
(*asserted by Plaintiff Carrozzella on behalf of the California Subclass*)

72. Plaintiff Carrozzella re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

73. Caesars and Plaintiff Carrozzella are "persons" as defined by the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17201.

74. The UCL states that "unfair competition shall mean and include any [1] unlawful, unfair or fraudulent business act or practice and [2] unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

75. By failing to take reasonable precautions to protect the PII of Plaintiff Carrozzella and the California Subclass, Caesars has engaged in "unlawful," "unfair," and "fraudulent" business practices in violation of the UCL.

76. First, Caesars engaged in "unlawful" acts or practices because it violated multiple laws, including but not limited to the California Consumer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures); the FTC Act, 15 U.S.C. § 45; and the common law, all as alleged herein.

77. Second, Caesars engaged in "unfair" acts or practices, including the following:

(a) Caesars failed to implement and maintain reasonable data security measures to protect the California Subclass members' PII. Caesars failed to identify foreseeable security risks, remediate identified risks, and adequately improve its data security in light of the highly sensitive nature of the data which it maintained and the known risk of cyber intrusions in the hospitality industry. Caesars' conduct, with little if any social utility, is unfair when weighed against the harm to the California Subclass members whose PII has been compromised.

(b) Caesars' failure to implement and maintain reasonable data security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' personal information and ensure that entities entrusted with PII adopt appropriate security measures. These policies are reflected in various laws, including but not limited to the FTC Act, 15 U.S.C. § 45; and the California Consumer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures).

(c) Caesars' failure to implement and maintain reasonable data security measures also led to substantial consumer injuries described herein, which are not outweighed by

countervailing benefits to consumers or to competition. Moreover, because consumers could not know of Caesars' inadequate data security, consumers could not have reasonably avoided the harms that Caesars' conduct caused.

78. Third, Caesars engaged in "fraudulent" acts or practices, including but not limited to the following:

(a) Caesars omitted and concealed the fact that it did not employ reasonable safeguards to protect consumers' PII. Caesars could and should have made a proper disclosure during the account creation process for Caesars Rewards members, or by any other means reasonably calculated to inform consumers of the inadequate data security. Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hospitality industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its data security was insufficient to guard against those attacks.

(b) Caesars also made implied or implicit false representations that its data security practices were sufficient to protect consumers' PII. Caesars required consumers to provide their PII—including Social Security and driver's license numbers—during Caesars Rewards account creation process. In doing so, Caesars made implied or implicit representations that its data security practices were sufficient to protect consumers' PII. By virtue of accepting Plaintiffs' PII during the Caesars Rewards account creation process, Caesars implicitly represented that its data security procedures were sufficient to safeguard the PII. Those representations were false and misleading.

79. Plaintiff Carrozzella and California Subclass members transacted with Caesars in California by, among other things, creating, using, and maintaining their Caesars Rewards accounts while in California. Plaintiff Carrozzella and California Subclass members were deceived in California when

they joined and used the Caesars Rewards program from California and were not informed of Caesars' deficient data security practices

80. As a direct and proximate result of Caesars' unfair, unlawful, and fraudulent acts and practices, Plaintiff Carrozzella and California Subclass members were injured, lost money or property, and suffered the various types of damages alleged herein.

81. The UCL states that an action may be brought by any person who has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff Carrozzella and California Subclass members suffered injury in fact and lost money or property as a result of Caesars' unfair competition including the loss of value of their breached PII. PII is valuable, which is demonstrated not only by the fact that Caesars requires consumers to provide PII during the Caesars Rewards account creation process, but also because Caesars uses PII for its marketing and other purposes.

82. Cal. Bus. & Prof. Code § 17203 states:

> Any person who engages, has engaged, or proposes to engage in unfair competition may be enjoined in any court of competent jurisdiction. The court may make such orders or judgments . . . as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition, as defined in this chapter, or as may be necessary to restore to any person in interest any money or property, real or personal, which may have been acquired by means of such unfair competition.

83. Plaintiff Carrozzella and California Subclass members are entitled to the injunctive relief requested herein to address Caesars' past and future acts of unfair competition.

84. Plaintiff Carrozzella and California Subclass members are entitled to restitution of money and property that was acquired by Caesars by means of its unfair competition and restitutionary disgorgement of all profits accruing to Caesars as a result of its unfair business practices.

85. Plaintiff Carrozzella and the California Subclass lack an adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages.

86. Further, if an injunction is not issued, Plaintiff and Subclass members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Plaintiff lacks an adequate remedy at law that will reasonably protect against the risk of such further breach.

87. Plaintiff Carrozzella and California Subclass members seek all monetary and non-monetary relief allowed by the UCL, including reasonable attorneys' fees under Cal. Code of Civ. Procedure § 1021.5.

COUNT III
VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code § 1798.80, et seq.
(*asserted by Plaintiff Carrozzella on behalf of the California Subclass*)

88. Plaintiff Carrozzella re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

89. The California legislature enacted the California Customer Records Act ("CCRA") to "ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5.

90. The CCRA states: "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain *reasonable security procedures and practices* appropriate to the nature of the information, to protect the personal information from unauthorized access." Cal. Civ. Code § 1798.81.5(b) (emphasis added).

91. The CCRA defines owns, licenses, and maintains as follows: "[T]he terms 'own' and 'license' include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term 'maintain' includes personal information that a business maintains but does not own or license.'" Cal. Civ. Code § 1798.81.5(a)(2). Caesars owns, licenses, and/or maintains the PII that was involved in the Data Breach.

92. The CCRA defines personal information as follows: "'Personal information' means either of the following: (A) An individual's first name or first initial and the individual's last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: . . . (i) Social security number (ii) Driver's license number . . .."

Cal. Civ. Code § 1798.81.5(d)(1). The PII stolen in the Data Breach includes personal information that meets this definition. The PII was unencrypted, as evidenced by the fact that Caesars was required to provide notification letters under the laws of several states that require notification of unauthorized access to unencrypted and unredacted information.

93. Caesars failed to maintain reasonable data security procedures appropriate to the nature of the PII. Accordingly, Caesars violated Cal. Civ. Code § 1798.81.5(b).

94. Plaintiff Carrozzella and California Subclass members were injured by Caesars' violation of Cal. Civ. Code § 1798.81.5(b) and seek damages pursuant to Cal. Civ. Code § 1798.84(b). They seek all monetary and non-monetary relief allowed by the CCRA to compensate for their various types of damages alleged herein.

95. Plaintiff Carrozzella and the California Subclass members have suffered injuries including but not limited to actual damages, and in being denied a statutory benefit conferred on them by the California legislature.

COUNT IV
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.100, et seq.
(*asserted by Plaintiff Carrozzella on behalf of the California Subclass*)

96. Plaintiff Carrozzella re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

97. Cal. Civ. Code § 1798.150(a)(1) provides that "Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action."

98. Plaintiff Carrozella and the members of the California Subclass are consumers as that term is defined in Cal. Civ. Code § 1798.140(i).

99. Caesars is a business as that term is defined in Cal. Civ. Code § 1798.140(d). Caesars is organized or operated for the profit or financial benefit of its owners. Caesars collects consumers' personal information (including Plaintiff Carrozzella and the members of the California Subclass) or such information is collected on Caesars' behalf, and Caesars determines the purposes and means of processing of consumers' personal information. Caesars does business in California and had annual revenue of billions of dollars in the preceding year.

100. The information compromised during the Data Breach constitutes "personal information" as that term is defined in Cal. Civ. Code § 1798.140(v)(1). At a minimum, that information included names, Social Security numbers, driver's license numbers, and dates of birth.

101. Under the CCPA, Caesars had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information that it stored. Cal. Civ. Code § 1798.150(a)(1).

102. Plaintiff Carrozzella's and the California Subclass members' nonencrypted and nonredacted personal information, as defined in Cal. Civ. Code § 1798.81.5(d)(1), was exfiltrated in the Caesars Data Breach, including names and Social Security and driver's license numbers.

103. Caesars violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Caesars' information security controls to ensure that PII in its possession was adequately secured by, for example, encrypting sensitive personal information, installing intrusion detection systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

104. Caesars knew or should have known that its computer systems and information security controls were inadequate to safeguard Plaintiff Carrozzella and Class members' PII and that unauthorized access and exfiltration, theft, or disclosures, was highly likely as a result. Caesars' actions in engaging in the above-named unlawful practices and acts were negligent, knowing, willful, and/or wanton and reckless with respect to the rights of Plaintiff Carrozzella and Subclass members.

105. As a direct and proximate result of the foregoing, Plaintiff Carrozzella and the California Subclass members have suffered injuries including but not limited to actual damages, and in being denied a statutory benefit conferred on them by the California legislature.

106. As a result of these violations, Plaintiff Carrozzella and the California Subclass members are entitled to actual pecuniary damages, injunctive or declaratory relief, and any other relief that the Court deems proper. Plaintiff reserves the right to amend this Complaint to seek statutory damages under the CCPA on behalf of himself and the Subclass after providing Caesars with the written notice required by Cal. Civ. Code § 1798.150(b).

COUNT V
NEGLIGENCE
(*asserted by all Plaintiffs on behalf of the Class*)

107. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

108. Plaintiffs and Class members were required to provide their PII, including their names, dates of birth, addresses, telephone numbers, email addresses, and drivers' license and Social Security numbers to Caesars as a condition of joining Caesars Rewards.

109. Plaintiffs and Class members entrusted their PII to Caesars with the understanding that Caesars would safeguard their PII.

110. In its written privacy policies, Caesars expressly promised Plaintiffs and Class members that it would only disclose PII under certain circumstances, none of which relate to the Caesars Data Breach. In addition, Caesars promised to maintain reasonable and appropriate safeguards to protect Plaintiffs' and Class members' PII.

111. Caesars had full knowledge of the sensitivity of the PII that it stored and the types of harm that Plaintiffs and Class members could and would suffer if that PII were wrongfully disclosed.

112. Caesars violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Caesars' information security controls to ensure that PII in its possession was adequately secured by, for example,

encrypting sensitive personal information, installing intrusion detection systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

113. Caesars' duty of care arose from, among other things,

(a) Caesars' exclusive ability (and Class members' inability) to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;

(b) Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;

(c) Caesars' common law duties to adopt reasonable data security measures to protect customer PII and to act as a reasonable and prudent person under the same or similar circumstances would act; and

(d) State statutes requiring reasonable data security measures, including Nev. Rev. Stat. § 603A.210, which states that businesses possessing personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from unauthorized access."

114. Caesars' violation of the FTC Act and state data security statutes constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs belong and to prevent the types of harm that resulted from the Data Breach.

115. Caesars is a multi-billion-dollar publicly traded company that had the financial and personnel resources necessary to prevent the Data Breach. Caesars nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiffs and Class members.

116. Plaintiffs and Class members were the foreseeable victims of Caesars' inadequate data security. Caesars knew that a breach of its systems could and would cause harm to Plaintiffs and Class members.

117. Caesar's conduct created a foreseeable risk of harm to Plaintiffs and Class members. Caesars' conduct included its failure to adequately restrict access to its loyalty program database that held consumers' PII.

118. Caesars knew or should have known of the inherent risks in collecting and storing massive amounts of PII, the importance of providing adequate data security over that PII, and the frequent cyberattacks within the hospitality industry.

119. Plaintiffs and Class members had no ability to protect their PII once it was in Caesars' possession and control. Caesars was in an exclusive position to protect against the harm suffered by Plaintiffs and Class members as a result of the Data Breach.

120. Caesars, through its actions and inactions, breached its duty owed to Plaintiffs and Class members by failing to exercise reasonable care in safeguarding their PII while it was in Caesars' possession and control. Caesars breached its duty by, among other things, its failure to adopt reasonable data security practices and its failure to adequately encrypt the PII in its systems.

121. Caesars inadequately safeguarded consumers' PII in deviation of standard industry rules, regulations, and best practices at the time of the Data Breach.

122. But for Caesars' breach of its duty to adequately protect Class members' PII, Class members' PII would not have been stolen.

123. There is a temporal and close causal connection between Caesars' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class members.

124. As a result of Caesars' negligence, Plaintiffs and Class members suffered and will continue to suffer the various types of damages alleged herein.

125. Plaintiffs and Class members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiffs and Class members are also entitled to the injunctive relief sought herein.

COUNT VI
NEGLIGENT MISREPRESENTATION
(*asserted by all Plaintiffs on behalf of the Class*)

126. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

127. Nevada has adopted the Restatement (Second) of Torts § 551 (1977), which imposes liability for negligent misrepresentations based on omissions. Section 551, titled "Liability for Nondisclosure," states:

> One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same liability to the other as though he had represented the nonexistence of the matter that he has failed to disclose, if . . . he is under a duty to the other to exercise reasonable care to disclose the matter in question.

128. Caesars failed to disclose to Plaintiffs and Class members that it did not employ reasonable measures to protect consumers' PII.

129. Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hospitality industry is a frequent target of sophisticated cyberattacks.

130. Caesars' omissions were material given the sensitivity of the PII maintained by Caesars and the gravity of the harm that could result from theft of the PII.

131. Caesars knew that consumers would create Caesars Rewards accounts under a mistake as to facts basic to the transactions. Because of the relationship between the parties, consumers would reasonably expect a disclosure of Caesars' inadequate data security.

132. Had Caesars disclosed its inadequate data security to Plaintiffs and Class members, Plaintiffs and Class members would not have entrusted their PII to Caesars.

133. Caesars should have made a proper disclosure to consumers during the Caesars Rewards account creation process, as part of the purchase of goods or services by Caesars Rewards members, or by any other means reasonably calculated to inform consumers of its inadequate data security.

134. In addition to its omissions, Caesars is also liable for its implied misrepresentations. Caesars required consumers to provide their PII during the Caesars Rewards account creation process. In doing so, Caesars made implied or implicit representations that it employed reasonable data security practices to protect consumers' PII. By virtue of accepting Plaintiffs' and Class members' PII during the Caesars Rewards account creation process, Caesars implicitly represented that its data security processes were sufficient to reasonably safeguard the PII. This constituted a negligent misrepresentation.

135. Caesars failed to exercise reasonable care or competence in communicating its omissions and misrepresentations.

136. As a direct and proximate result of Caesars' omissions and misrepresentations, Plaintiffs and Class members suffered the various types of damages alleged herein.

137. Plaintiffs and Class members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

COUNT VII
UNJUST ENRICHMENT
(*asserted by all Plaintiffs on behalf of the Class*)

138. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

139. Plaintiffs and Class members conferred a monetary benefit upon Caesars. Specifically, they provided their PII to Caesars, which Caesars used for marketing and other revenue-generating purposes. Caesars used its rewards program to incentivize Class members to spend money on hotel stays, gambling, dining, entertainment, and other services at Caesars properties.

140. In exchange for providing PII to Caesars, Plaintiffs and Class members should have received their Caesars Rewards membership and associated benefits accompanied by adequate safeguarding of their PII.

141. Under principles of equity and good conscience, Caesars should not be permitted to retain the full monetary benefit of its transactions with Plaintiffs and Class members, because Caesars failed to adequately secure consumers' PII and, therefore, did not provide the full services that consumers transacted for.

142. Caesars acquired consumers' PII through inequitable means in that it failed to disclose its inadequate data security practices when entering into transactions with consumers and obtaining their PII.

143. If Plaintiffs and Class members would have known that Caesars employed inadequate data security safeguards, they would not have agreed to transact with Caesars.

144. Plaintiffs and Class members have no adequate remedy at law. Caesars continues to retain Class members' PII while exposing the PII to a risk of future data breaches while in Caesars' possession. Caesars also continues to derive a financial benefit from using Class members' PII.

145. As a direct and proximate result of Caesars' conduct, Plaintiffs and Class members have suffered the various types of damages alleged herein.

146. Caesars should be compelled to disgorge into a common fund or constructive trust, for the benefit of Class members, the proceeds that they unjustly derived from use of Class members' PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully request the following relief:

a. An Order certifying this case as a class action with the class definition provided herein, and appointing Plaintiffs and Plaintiffs' identified counsel to represent the Class and appointing Plaintiff Carrozzella and his counsel to represent the California Subclass;

b. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Class members' PII;

c. A mandatory injunction directing Caesars to adequately safeguard the PII of Plaintiffs and the Class by implementing improved security controls;

d. Restitution, disgorgement, and other appropriate equitable relief;

e. An award of compensatory, statutory, and punitive damages, as appropriate, in an amount to be determined;

f. Declaratory relief stating that Caesars failed to meet applicable information security standards, statutory and common law duties, and other obligations regarding Plaintiffs' and the Class members' PII, and that such failure actually and proximately caused damage to

Plaintiffs, the Class, and the Subclass;

g. An award of costs and litigation expenses;

h. An award of attorneys' fees; and

i. Such other and further relief, injunctive and otherwise, as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial as to all issues so triable.

Dated this 23rd day of October, 2023.

CLAGGETT & SYKES LAW FIRM

/s/ Micah Echols

Micah S. Echols, Esq.
Nevada Bar No. 8437

GIBBS LAW GROUP LLP
David M. Berger (*pro hac vice to be submitted*)
Jeffrey B. Kosbie (*pro hac vice to be submitted*)
Julia L. Gonzalez (*pro hac vice to be submitted*)
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9700
Facsimile: (510) 350-9701
dmb@classlawgroup.com
jbk@classlawgroup.com
jlg@classlawgroup.com

ATTORNEYS FOR PLAINTIFFS MICHAEL CARROZELLA, FRANK ANDERSON, GREG LEWIS, AND THE PROPOSED CLASSES